Audit and Risk Assurance Committee

Minutes of the meeting of the Audit and Risk Assurance Committee held in public on:

Date:	Wednesday 19 June 2024
Time:	2pm
Venue:	Videoconference (Microsoft Teams)
Members:	Lianne Patterson (Chair) Helen Gough (until item 9) Graham Masters David Stirling
Apologies:	Jordan McKenna[*]
Attendees:	Aihab Al-Koubaisi, Financial Controller Francesca Bramley, Governance Manager Alastair Bridges, Executive Director of Resources Heather Buckingham, BDO LLP Kathryn Burton, Haysmacintyre LLP Roy Dunn, Chief Information Security and Risk Officer Karen Flaherty, Head of Governance Nicole Jones, Compliance Officer Alan Keshtmand, Head of Finance Geraldine Kinkead-Richards, Council Apprentice Geoff Kirk, Head of IT and Digital Transformation (for item 8) Anna Raftery, Head of Assurance and Compliance Daniel Reay, National Audit Office (NAO) Gareth Roberts, NAO Andrew Smith, Executive Director of Education, Registration and Regulatory Standards and Deputy Chief Executive

[*] Council Apprentice

1. Welcome and introduction

1.1. The Chair welcomed those present to the meeting of the Audit and Risk Assurance Committee (the Committee) and extended a particular welcome to Helen Gough who was attending her first meeting as a member of the Committee.

2. Apologies for absence

2.1. Apologies were received from Jordan McKenna, the Council Apprentice who would usually attend meetings of the Committee.

3. Approval of agenda

3.1. The Committee approved the agenda.

4. Declarations of members' interests in relation to agenda items

4.1. No interests were declared.

5. Minutes of the Audit and Risk Assurance Committee meeting held in public on 13 March 2024

5.1. The Committee approved the minutes of the meeting of the Committee held in public on 13 March 2024 as an accurate record of that meeting.

6. Matters arising

6.1. The Committee noted the updates provided in response to the actions from its previous meeting.

7. Strategic risk register

7.1. The Committee reviewed the latest version of the Strategic Risk Register (SRR). It was noted that the review date shown in the SRR should have been May 2024 not February 2024. There had been no changes to the risk ratings since the SRR was last reviewed by the Committee at its meeting in March 2024.

7.2. It was clarified that the RAG rating for the current risk level for strategic risk 5 (having sustainable resources to achieve our strategy in place) should have reflected that this risk was not within the risk appetite as described in the narrative. There had been some discussion about reducing the risk rating following the fee increase implemented in November 2023, however, it was felt that this would not be appropriate until more regular fee reviews were implemented to put the HCPC on a more financially sustainable footing.

7.3. The work to introduce measures to monitor how mitigations were contributing to improving the risk assurance rating and reaching the target risk score in the SRR was continuing. The mitigations were currently being updated to reflect the corporate plan for 2024-25. The current risk and assurance review meetings confirmed that there had been further positive improvement with the planned mitigations, however, this had not yet resulted in any significant changes to assurance ratings or risk scores.

7.4. The Committee discussed how the strategic risk to harness the benefits of the data held by the HCPC (strategic risk 3) needed to be addressed by both improvements in the quality of the data and mechanisms to share data effectively with the relevant stakeholders. There was a degree of overlap with strategic risk 4 relating to engaging with stakeholders, and the mitigations in place, however, the need to deliver both aspects in order to address the risk and achieve the target risk score for strategic risk 3 was acknowledged.

8. Strategic risk deep dive: cybersecurity

8.1. The Head of IT and Digital Transformation joined the meeting for this item. The Chief Information Security and Risk Officer gave a presentation about the strategic risks relating to cybersecurity within the HCPC, an area of risk that had been raised by the Committee during its workshop in February 2024.

8.2. The presentation covered the following areas:

- the external factors resulting in an increased risk of cyberattack generally, including international conflicts, motivation, greater use of automation, technical expertise and the transition to storage of data in the cloud, although the value of global ransomware attacks had decreased in recent years following a peak in 2021;

- the information security related data losses at the HCPC, which were mostly due to the information being sent to the wrong individual or personal data not being correctly redacted before information was shared and how these were reported and responded to;

- the methods and vulnerabilities used for cyberattacks, including the use of AI technologies and risks related to suppliers;

- the work plan for 2024-25 to classify documents, emails and data and apply rules based on those classifications to prevent data loss, while still ensuring that the HCPC functioned effectively and introducing more robust requirements and audits of suppliers in relation to information security;

- the partial adoption of the National Institute of Standards and Technology (NIST) framework, which was a more detailed US government framework similar to the ISO27001 standard;

- the monitoring and benchmarking of the HCPC's performance against the Microsoft Defender and Secure scores, which were reported to the People and Resources Committee at each meeting and demonstrated performance above the industry average; and

- the strategic and operational risks specifically relating to cybersecurity.

8.3. The Committee considered the cultural issues underpinning information security and ensuring that rules and methods of classification were interpreted and applied consistently. While the classification of information with clear definitions based on ISO27001 had been in place at the HCPC for a number of years, the changes being introduced would apply rules to those classifications. Some departments, such as Fitness to Practise (FTP) and Registration, already had rules in place around the classifications. The rules that would apply to the four different classifications were being put in place in consultation with different areas of the organisation to understand the impact on those areas prior to implementation. Some of these rules would highlight where information was confidential and prompt employees to consider and take action. This would also highlight to managers where rules were not followed.

8.4. The Committee discussed risk ownership at a corporate level and for specific data and policies, as some risks had the Head of IT and Digital Transformation and the Chief Information Security and Risk Officer as risk owners, whereas the relevant information asset owner had responsibility for other risks.

9. Annual Information Governance Report 2023-24

9.1. The Committee noted the annual information governance report for the period from 1 April 2023 to 31 March 2024.

9.2. The increase in the number of requests for information and challenges through the internal review process was linked to the increase in the number of FTP referrals and investigations. It was noted that the HCPC's approach to responding to requests for information under the Freedom of Information Act 2000 (FOI) about FTP concerns and investigations prior to consideration by an Investigating Committee Panel, by neither confirming or denying that it held the information, had been endorsed by the Information Commissioner's Office and the First-tier Tribunal following an appeal.

Action: Given the small number of late responses to FOI requests (nine in total), it was requested that the number of requests as well as the percentage was included in future reports when providing any breakdown of the reasons for this.

9.3. The Committee discussed whether processes and other human factors had been considered in the information incidents where the cause was recorded as human error; which was the main cause of these incidents. Some of the incidents recorded as human error could be categorised as the process not having been followed or the process having failed to better understand whether there was something in the process that could be changed to support people to follow this or to highlight more quickly when a process was not followed. Individuals were encouraged to report incidents, including an explanation of the reasons that the incident occurred and any actions that could prevent a similar incident reoccurring.

Action: The Head of Assurance and Compliance would work with the Chief Information Security and Risk Officer to review the categorisation and the reasons for these incidents and ways to identify and address the underlying causes of these.

9.4. The Committee questioned whether some of the FOI requests could be addressed using a self-service approach by making more registration and other data available online with better search functionality. Based on the experience of the General Medical Council, which had made similar data and search tools available online, this could potentially address 45% of FOI requests. There would still be a number of requests that would need to be responded to individually as these were seeking more detail than would be available online. The Executive Director of Education, Registration and Regulatory Standards was championing a move to greater use of self-service and making data available at regular reporting intervals, which would offer efficiency benefits even when responding to individual, more detailed requests.

9.5. The Committee noted the approach to entering into memoranda of understanding (MOU) with larger third party organisations to facilitate disclosure of information, although these were not strictly necessary given the HCPC’s powers and duties to disclose information under applicable legislation.

10. Unified assurance annual summary 2023-24

10.1. The Head of Assurance and Compliance presented the annual summary of the unified assurance framework for 2023-24. More detail was included in the unified assurance report to be considered in the private session of the meeting.

10.2. The annual report illustrated the progress and improvement during 2023-24 with the increase in the number and percentage of processes moving into higher levels of assurance. At the end of 2023-24 the overall assurance rating had improved from ‘Medium’ to ‘High/Medium’.

10.3. There were two areas with ‘Medium/Low’ assurance consistently throughout the year, however, significant work was ongoing to address the concerns and it was taking time to realise and assess the impact of the improvements made. Close monitoring was in place for these areas as an additional control.

11. Internal audit progress report

11.1. The Committee noted the internal audit progress report, updating on the delivery of the internal audit plan for 2024-25, and noted that no reviews had yet been completed given the early stage in the year. The link to BDO’s Global risk landscape report in the progress report was highlighted and members of the Committee were encouraged to read this.

11.2. The fieldwork was in progress for the Education – new approach and Key Performance Measures internal audits and the terms of reference for the Stakeholder Engagement and Environmental Sustainability internal audits were in the process of being agreed. The scoping of the Health and Safety and Data Privacy internal audits would commence over the next couple of months.

12. Internal Audit Annual Report and Opinion 2023-24

12.1. The Committee noted the final internal audit annual report and opinion for 2023-24, which had been presented in draft at the meeting of the Committee in March 2024.

12.2. There had been no changes to the internal audit annual report or opinion since the draft was presented and the opinion provided a moderate rating, the second highest rating, which indicated that there was some risk that the system of internal control, governance and risk management would fail to meet management's objectives, with some areas where there were adequate and effective systems of governance, but also some specific areas of significant risk. Significant improvements were required in specific areas to improve the adequacy or effectiveness of governance, risk management and internal control.

12.3. The Chair noted that the Committee had advised by the internal auditor at its last Committee meeting in March 2024 that the HCPC was comfortably within the moderate rating band. It also agreed that the HCPC should continue to aspire to achieve the highest rating of substantial.

13. Internal audit recommendations tracker

13.1. The Committee noted the updates on the implementation of recommendations arising from internal audits. The tracker now included updates for each recommendation, including explanations where there was no progress to report, as requested by the Committee at its previous meeting.

Actions:

a. The Executive Director of Education, Registration and Regulatory Standards would provide further granularity for the Committee about the progress of the recommendation relating to policies, procedures and guidance, in response to the internal audit of regulatory policy. This would also be included in the next update and would include a description of the document(s) being produced and the plan to create or update this.

b. The commentary in the internal audit recommendations tracker should also give an indication of whether the recommendations had or would be completed by the agreed timescale.

14. Audit planning report 2023-24

14.1. The Committee received a report from the NAO confirming the proposed approach for the audit of the 2023-24 financial statements of the HCPC and setting out its assessment of risks and materiality. The report also included details of the team carrying out the audit, the timing of the audit and the fees for the audit.

14.2. The three risks of material misstatement or irregularity within transactions and balances identified by the NAO as impacting on its audit were:

- presumed risk of management override of controls;
- risk of fraud in revenue recognition; and
- valuation of land and buildings.

These were consistent with the areas of risk in prior years and there were no new risks identified. Two areas of risk that had diminished since the audit of the 2022-23 financial statements were implementation of IFRS 16 relating to leases and the provision relating to the Nursing and Midwifery Council and Somerville case. The latter risk would be kept under review during the audit. The areas of audit focus for the NAO were completeness of creditors and completeness of staff costs.

14.3. In line with the approach of the HCPC’s external auditor, Haysmacintyre LLP (HM), the quantitative materiality threshold for the audit had been set as approximately 2% of 2022-23 income, giving a planning materiality of £741,000. This was slightly higher than the 2022-23 threshold, however, the basis on which this was set had not changed. The NAO would also consider materiality qualitatively, and in areas that were particularly sensitive to inaccuracy or omission misstatements might be treated as material and reported to the Committee even where these were below the quantitative threshold.

14.4. The audit fee of £13,000 was based on the anticipated cost of delivering the audit and was broadly in line with the fee for the previous year’s audit.

14.5. The Committee considered and agreed that:

- the NAO’s assessment of the risks of material misstatement to the financial statements was complete from its perspective;
- management’s response to the risks of material misstatement were adequate;
- the proposed audit plan addressed these risks;
- it did not believe that the financial statements could be materially misstated due to fraud and there were no areas of concern that it wished to communicate to management or the audit team;
- there were no other matters that it believed might influence the audit of the financial statements;
- it was not aware of any business risks related to the HCPC’s objectives and strategies that might result in material misstatements;
- there were processes in place for identifying and responding to the risks of fraud;
- no non-compliance with any laws or regulations had been reported to it and policies, procedures and systems for recording non-compliance were in place; and
- members did not have knowledge of any actual, suspected or alleged fraud affecting the HCPC.

14.6. The Committee approved the approach, timing and fee for the audit of the 2023-24 financial statements of the HCPC.

15. External audit update

15.1. The Committee received a verbal update from the external auditor, HM, about the progress of the external audit. Its fieldwork was due to commence on 8 July 2024. The response to its requests for data had been good and there had been regular communication. There were currently no concerns about the timetable or provision of information.

15.2. The Committee thanked the Finance team for responding so well to requests for information from the external auditor and maintaining good communication.

16. Annual report and accounts 2023-24 update including draft annual report 2023-24

16.1. The Committee reviewed the draft annual report, focussing on identifying any gaps in the key messages, themes and/or tone of the narrative in order to ensure that the annual report was fair, balanced and understandable.

16.2. The Governance Manager was thanked for her work coordinating and compiling the information in the annual report. The inputs to the annual report had been received on time, with only a couple of areas yet to be included:

- the information relating to FTP, which was being compiled for the FTP annual report 2023-24; and
- the commentary on internal controls and risks, including the results of the Professional Standards Authority's 2023-24 performance review while awaiting the final outcome and report.

16.3. The Committee was satisfied with the key messages and themes in the annual report and had not identified any gaps. The Chair requested that the information in the different sections was reviewed once complete to ensure that there was an appropriate balance and emphasis in areas of equivalent significance.

16.4. The preparation of the financial statements was progressing well and a draft would be sent to HM by 28 June 2024 as planned. A further draft of the annual report, incorporating the financial statements, would be shared with Committee members by email in July 2024.

Action: Committee members agreed to provide any specific feedback on areas of the annual report, including any typographical errors that they had spotted during their review by 4 July 2024.

17. Audit and Risk Assurance Committee annual report to the Council and the Accounting Officer 2023-24

17.1. The Committee reviewed and approved the Committee's annual report to the Council and the Accounting Officer for 2023-24, which was included as part of the governance statement within the annual report and accounts.

18. Resolution to move the meeting to private session

18.1. The Committee resolved that the remainder of the meeting would be held in private because the matters being discussed related to:

- matters which, in the opinion of the Chair, were confidential or the public disclosure of which would prejudice the effective discharge of the Committee’s or Council’s functions;

- action being taken to prevent or detect crime or to prosecute offenders in the case of item 22; or

- the terms of, or expenditure under, a tender or contract for the purchase or supply of goods or services in the case of item 23.

The meeting was briefly adjourned.